Panabit 流控管理配置手册

(核心代号 shang，V8.05)

北京三棱镜软件工作室

2008.06

目 录

目 录 2
前言 3
0. 系统检查 4
0.1 确认系统时间 4
0.2 查看数据网卡POLLING选项 4
0.3 关闭CPU超线程 4
0.4 配置与测试网桥 5
0.5 修改口令 5
1. 网络配置 5
1.1 管理接口 6
1.2 数据接口 7
2. 对象管理 7
2.1 自定义协议 7
2.2 IP群组 8
2.3 自定义协议组 9
3. 流量管理 9
3.1 网桥带宽 9
3.2 内网IP统计 10
3.3 数据通道 11
3.4 策略组 11
3.5 策略调度 17
4. 监控统计 19
4.1 分桥统计 19
4.2 网络接口 20
4.3 应用协议 20
5. 系统维护 21
附录 22
P2P下载控制 22
迅雷、超级旋风控制示例 22
Panabit应用协议样本抓包方法 24

前言

感谢您使用 Panabit 流控产品！

Panabit 应用层流量管理产品，是在互联网 P2P(Peer-to-Peer)应用广泛流行的背景下，诞生的新一代应用层 QOS 产品。Panabit 流控是真正一款应用层级流控产品，基于连接过程和协议特征识别，对于加密协议采用主动探测引擎，经过一套完整的识别流程，准确识别应用，精确定位具体的软件客户端，把应用可视化提高到一个新的阶段。Panabit 流控系统能帮助宽带运营网管实时了解网络应用层流量状态及应用概况，进行流量管理，提高网络运行效率。

流控产品，是一个典型的服务型产品，需要根据互联网应用的变化，不断改进协议识别引擎和更新协议特征库，才能保证流控的效果。应用层协议识别的重点和难点是 P2P 应用，P2P 流控是应用层流控的核心；互联网不断有新增加的应用，已有的应用为了逃避流控设备监管，采用技术对抗方法，伪装和变换协议特征，甚至整个趋势向加密方向发展，这使得流控产品的技术要跟踪、适应或超越这些变化，才能为用户提供良好的服务。

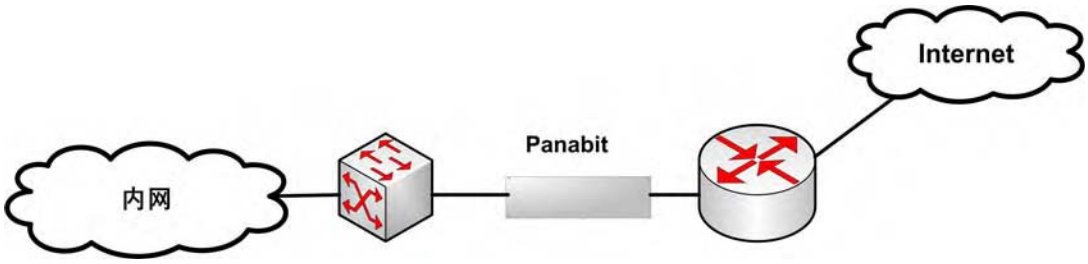
Panabit 流控产品，为了适应互联网应用的快速变化，有专门的研发团队跟踪研究，采用抓包的方法不断收集分析协议样本，利用自主开发、描述能力强的“协议特征描述语言”—PSDL(Protocol Signature Description Language)，维护协议特征库，快速提供给用户升级。Panabit 流控引擎，系统升级正常 3 个月升级一次版本，1 个月升级一次协议特征库，升级了特征库，将有更多的协议被识别，降低未知流量的比例。请 Panabit 流控产品用户，经常检查最新版本和最新特征库，尽量升级到最新版本，从而获得更好的流控效果。

在使用过程中，如果发现某个应用未能被正确识别，可以及时反馈或直接帮助采集样本，Panabit 在分析获取特征之后添加到协议特征库，通过特征库升级，就能及时解决问题。

Panabit 流控产品，全中文化的 Web 界面，界面简洁，操作容易掌握，必要的提示在 Web 界面中已经标明，可以脱离手册操作，但是还是建议，正式上线前，仔细阅读本手册，掌握策略配置的核心思想和流程，从而获得灵活的策略配置管理效果。

流量管理策略配置流程是：设定数据通道(划分通道，设定带宽值)—>定义策略组(添加规则集，规则按序号由小到大执行)—>策略调度(设定策略生效时间段)；确认当前生效策略，点击：监控统计—>当前策略。日常的维护主要是查看运行数据，适当调整策略。

Panabit 流控系统部署图如下：



注：本手册未包含软件安装部分，请参考 Panabit 安装指南。

0. 系统检查

旧版本升级的用户，可以直接跳至第 1 章节。

新装软件用户，需要对系统做进一步的检查与配置。

0.1 确认系统时间

系统安装时，给定了管理网口的 IP 地址信息，在浏览地址栏输入：

https://192.168.0.8　　（根据实际地址输入）

对于 IE 7.0，点击“继续浏览此网站(不推荐)”，则进入 Panabit 流控系统管理界面，管理员用户名是：admin，缺省口令是：panabit ；选择系统维护—>系统时间，确认时间正确；修改时间也可以在 FreeBSD 命令行修改，使用 date 命令调整，date 命令格式：date YYMMDDHHMM，如设置时间为 2008 年 06 月 23 日 18 点 30 分，则命令格式：date 0806231830，输入 date 命令，确认时间调整正确。如系统时间不正确，将影响系统的策略执行和流量图表统计信息。

0.2 查看数据网卡 POLLING 选项

对于硬件配置比较低，流量比较高的网络环境，需要设置 POLLING 选项，有利于提高网卡性能和降低 CPU 的负荷。

对于使用 Panabit 裁减的 FreeBSD 精简包安装的系统，内核已支持 POLLING 选项，启用 POLLING 选项，还需要在系统命令行配置，设置格式如下：

ifconfig fxp0 polling

ifconfig fxp1 polling

Polling 仅需对所有使用的数据接口设置，建议将设置添加到/etc/rc.local 文件中，使得开机进入系统自动运行。

对于自编译内核未增加 POLLING 选项的，参考 FreeBSD 6.2 系统安装文档的内核编译部分，启用新编译内核之后，设置方法同上。

使用 ifconfig 命令查看网卡信息，看到网卡后面有 POLLING 显示，说明已经打开 POLLING。

0.3 关闭 CPU 超线程

在系统信息—>CPU 配置一行，显示 CPU 信息，“(2)”表示双核。Panabit 流控引擎，目前仅支持双核，目前不支持 4 核。

Panabit 系统不使用超线程，如果主板支持超线程，在 bios 中关闭超线程(Hyper-Threading)，如果打开了超线程，数据网卡将不通流量。

0.4 配置与测试网桥

Panabit 系统，可以支持 4 路网桥的分别管理和统计流量；系统安装完毕，需要在 Web 管理界面设定网桥，网桥名称以网桥 1、网桥 2、网桥 3、网桥 4 标识，需要分别设置所使用的网卡和内外网接口，配置界面如下：

网络设置->数据接口　　系统已连续运行0天0小

接口名称	应用模式	接入位置	驱动类型	状态	操作
em1	网桥1	接外网	BSD	正常	提交
em2	网桥1	接内网	BSD	正常	提交
em3	网桥2	接外网	BSD	正常	提交
em4	网桥2	接内网	BSD	正常	提交

选网桥名称，设置接内网和外网，依次点击提交，网桥配置完成，即可上线开始流量分析，根据流量分析的结果，再配置管理策略。

上线前，须测试网桥是否正常，多路网桥，每一路都需要测试。简单的测试方法，将 Panabit 系统串接在笔记本电脑前上网，使用迅雷下载大文件，查看网络速度是否正常和迅雷是否被分析识别。测试正常后，设备即可正式上线。

0.5 修改口令

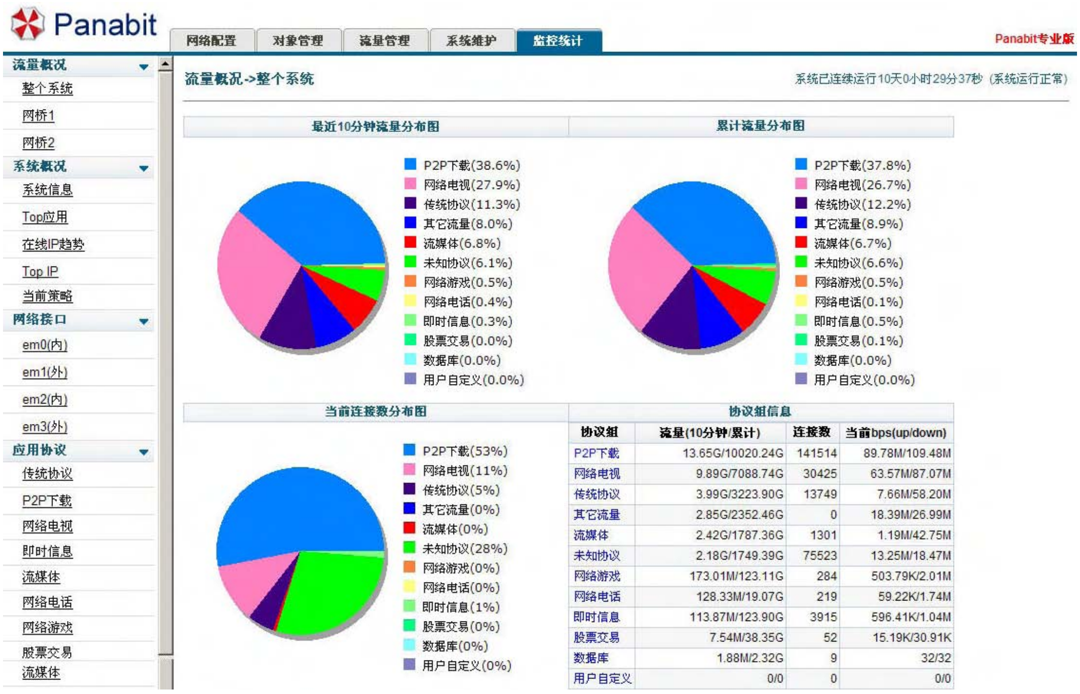
修改系统 root 帐户口令与 Web 界面 admin 管理帐户口令；需要设置复杂、足够强度的口令。

1. 网络配置

Panabit流控系统登录管理界面的方式是：https://192.168.0.8 。软件系统无缺省地址，是在安装时设定的管理接口IP地址，管理员用户名是：admin，缺省口令是：panabit。

如果系统管理密码丢失或未知管理 IP 地址，配置有串口终端的，可以通过 console 口登录修改密码和设置临时 IP 地址，Web 界面登录之后，通过 Web 界面配置和保存 IP 地址。参照 Panabit 精简包安装的 FreeBSD 系统，超级终端连接参数：9600 8 无 1 无 ，(点“缺省”即可)。

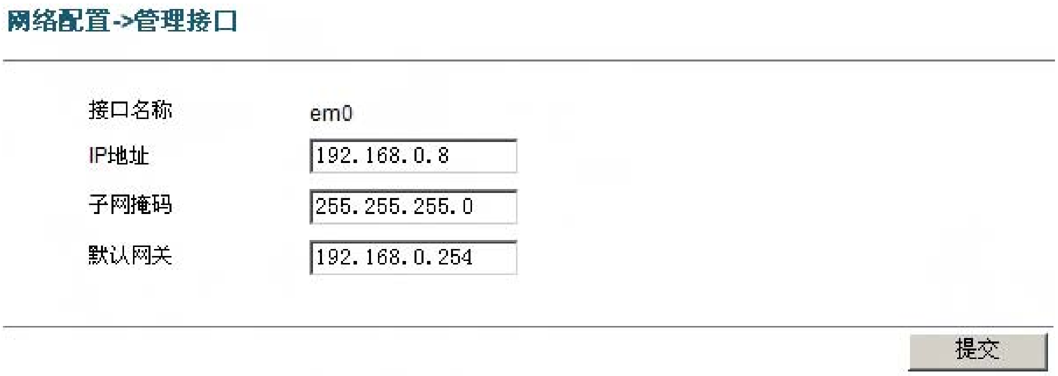
由于使用了安全登录，IE 7.0 登录管理界面时，出现安全警告提示页面，点击 “继续浏览此网站(不推荐)”，则进入 Panabit 流控系统管理界面，首页页面如下：



初始登录，由于无流量数据，饼图显示为灰色。

1.1 管理接口

修改管理接口 IP 界面如下：



修改完毕点击提交，管理接口 IP 地址修改生效并保存配置文件。

注：Panabit 的网络配置信息，使用单独的配置文件，FreeBSD 系统配置的网络信息，在启动 Panabit 进程时，将被 Panabit 网络配置信息替换，如果在系统命令行修改 Panabit 的管理地址信息，可以直接修改：/usr/panaetc/ifadmin.conf 文件，重启 Panabit 使其生效。可以在 FreeBSD 命令行用 ifconfig 临时修改管理接口 IP 地址，保存地址信息，需要到 Web 管理界面修改保存。

1.2 数据接口

网桥配置与察看界面如下：

网络设置->数据接口　　　系统已连续运行0天0小

接口名称	应用模式	接入位置	驱动类型	状态	操作
em1	网桥1	接外网	BSD	正常	提交
em2	网桥1	接内网	BSD	正常	提交
em3	网桥2	接外网	BSD	正常	提交
em4	网桥2	接内网	BSD	正常	提交

网桥的内外网接口，请根据硬件接口标识，不能接反；如果接反，将直接影响策略效果和流量统计信息。

上线前，需测试网桥是否正常，多路网桥，每一路都需要测试。简单的测试方法，将 Panabit 系统串接在笔记本电脑前上网，使用迅雷下载大文件，查看速度是否正常和迅雷是否被分析识别。测试正常后，即可正式上线测试。

上线后，系统先要保证网络的正常使用，不配置策略以纯桥方式进行流量分析，流量分析是逐步进行，初始时未知比例会很大并逐渐下降；通常 24 小时之后，各类流量比例才会趋于稳定，此时再根据流量分布比例，开始配置流量管理策略。策略设置好后的一周内，需要根据网络的实际运行情况和用户反馈状况做适当的调整直至恰当为止。

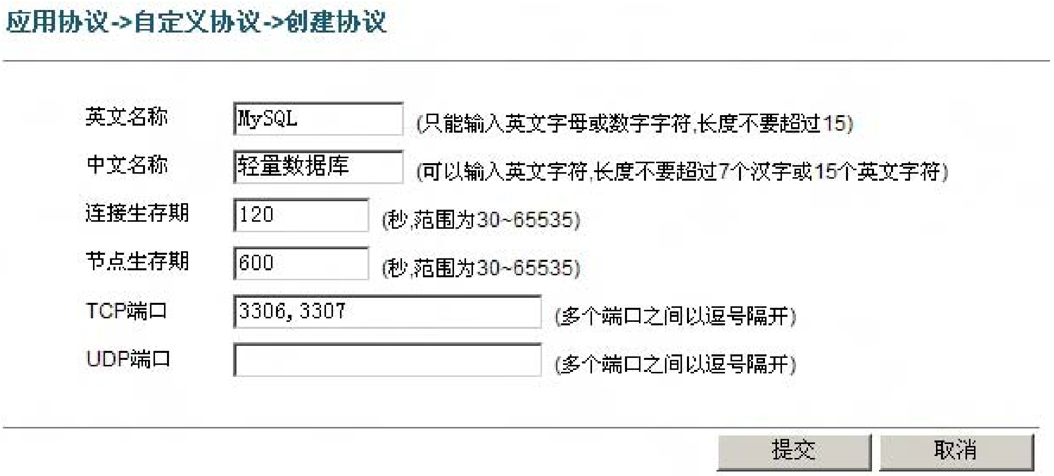
2. 对象管理

Panabit 流控管理，策略配置是基于对象、选项参数、动作组成具体的规则。

对象管理的功能是为了扩展自定义对象，Panabit 系统的基本对象已经包含：协议/协议组、源地址/目的地址。为了方便策略配置，可以根据实际情况自定义对象。可自定义对象包括：自定义协议、IP 群组、自定义协议组。

2.1 自定义协议

Panabit V8.05 版本，提供了基于端口的自定义协议。基于协议特征的自定义协议，由于挑选特征需要专业技巧，未提供特征类型的自定义。自定义协议界面和示例如下：



2.2 IP 群组

单 IP、IP 段在策略规则配置时，已经是可以作为控制对象的参数使用，但是一个 IP 地址或一个 IP 段，需要一条规则对应，对多个 IP 或 IP 段配置同一控制策略时，需要配置多条规则，操作起来比较烦琐，使用 IP 群组自定义功能，可以把多个 IP、不连续的 IP 段定义一个 IP 群组，并以组名称标识，这样配置策略方便和直观。

其它对象->IP群组

(所有群组)	起始地址	结束地址	创建群组>>
学生宿舍区	192.168.2.1	192.168.10.254	删除IP段
学生宿舍区	172.16.1.1	172.16.1.100	删除IP段
服务器	202.99.11.120	202.99.11.120	删除IP段
办公区	192.168.0.1	192.168.0.128	删除IP段
VIP	192.168.0.200	192.168.0.220	删除IP段
学生宿舍区			新增IP段

自定义 IP 群组之后，在策略配置规则时，组名称将自动添加到内网、外网地址对象中，供调用。

2.3 自定义协议组

Panabit 流控系统，已经根据客户端应用的功能，划分了 P2P 下载、网络电视、传统协议、网络游戏等大类，每个类别下面，再细分具体的协议名称。为了配置策略方便，可以把用户关注的协议（协议来自系统缺省分类的各个组别或自定义的协议），自定义为协议组。配置界面和示例如下：

迅雷正常使用的协议，组别是在 P2P 下载类，但迅雷又同时使用和支持其他协议，如果需要对迅雷下载所使用的各协议统一控制，将迅雷支持和使用的协议捆绑在一个迅雷系协议组，当配置对整个迅雷控制策略规则时就比较方便。通过 Panabit 流控系统 Web 管理界面监控统计，如查看单 IP 明细，看到迅雷还使用了 FTP 协议，则在上述自定义协议组中加入 FTP 协议。

3. 流量管理

流量管理项是 Panabit 流控系统实现流控管理的策略管理控制中心，策略配置、策略生效时间调度都在此部分进行。

在开始进行流量管理配置策略前，网桥带宽和内网 IP 统计两个选项需要设置，参照如下说明选择使用。

3.1 网桥带宽

网桥带宽是设定承载该链路的带宽最大值，对于策略中启用带宽预留、带宽保证时，需要设置

该值；对于策略中通常的允许、阻断、限速，忽略此值，系统缺省 0 值，即关闭上下行带宽预留、带宽保证功能。

不同的网桥，需要根据实际情况设置带宽，上下行分别设置。设置界面和示例如下：

3.2 内网 IP 统计

内网 IP 统计，是设置系统记录并统计当前在线 IP 的流量信息，由于开启内网 IP 流量统计功能影响系统资源开销，对于运营商级负载重的网络和硬件配置比较低的系统，不建议打开此选项，系统默认是关闭状态。

系统仅统计和显示当前的 IP 使用的协议和带宽使用状态，不保存此项信息，可以根据实际需要选择打开和关闭。开启或关闭内网 IP 统计设置界面和示例如下：

内网 IP 最大空闲时间缺省为 30 分钟，超过 30 分钟无流量的 IP 将从统计列表中被清除，建议

使用默认值。

3.3 数据通道

Panabit 流控系统，带宽管理策略配置分三步骤完成：1、定义数据通道(分配带宽数值)； 2、编辑策略组(控制规则集合)；3、定义策略调度表(策略生效)。如果仅配置允许、阻断策略，直接编辑策略组，仅 2、3 步骤即可。

数据通道设置比较简单，主要设置数据通道带宽数值和匹配的通道路径，当设置带宽预留、带宽保证时，可以选择带宽所在路径；对于带宽限速，无所在路径选项。设置数据通道的目的，是在策略组配置规则时作为执行动作使用，缺省的执行动作仅阻断和允许两项，一旦配置了数据通道，通道名称将加入执行动作选项，从而实现划分数据通道的目的。在自定义通道名称时，注意通道名称便于理解。

数据通道配置界面和示例如下：

控制策略->数据通道　　系统已连续:

通道名称	通道类型	通道路径	通道带宽(kb/s)	添加数据通道>>
limit-up	带宽限制	任意	25000	编辑 删除
limit-down	带宽限制	任意	60000	编辑 删除
nettv-up	带宽限制	任意	20000	编辑 删除
nettv-down	带宽限制	任意	100000	编辑 删除
预留3M-up	带宽预留	网桥1->上行	3000	编辑 删除
预留3M-down	带宽预留	网桥1->下行	3000	编辑 删除
web视频-up	带宽限制	任意	20000	编辑 删除
web视频-down	带宽限制	任意	60000	编辑 删除

以上数据通道名称，在接下来的策略组－>添加规则配置界面中，下拉“执行动作”选项，将出现新增加的数据通道名称，即数据通道是为策略配置先行设置的动作。

通道表示为带宽数值，一个已经定义的数据通道，在规则配置中可以灵活使用，可以表示上行、下行、双向、协议总和、网桥总和，即数据通道可以共用。

关于带宽预留、带宽保证通道：

带宽预留－－对于预留的对象，最大可以使用预留带宽。

带宽保证－－对于保证对象，至少保证的带宽，系统带宽空闲，还可以借用。

3.4 策略组

1）创建策略组并为其命名

策略组是控制规则的集合，策略组创建之后，逐一添加规则；根据实际需要，可以创建多个策略组，供不同时间段调用；

2）点击“添加规则”创建规则

注：配置界面各参数后面括号中蓝色部分为相关的注释，将鼠标移动到蓝色字体部分即可显示相关说明。

本例为创建一个编号为 20 的规则。

规则编号，是自定义的序号，是策略执行的顺序，有小到大执行，实际在编号时，编号之间留些空档，便于插入规则，如 10、20、30 这样编号，如果在 10－20 之间插入新的规则，就有编号可用，如果预计插入的规则较多，编号间隔加大。

“数据路径”：表示本规则作用链路的范围。“任意路径”表示该规则作用于整个系统所有网桥的任意方向；“任意上/下行路径”表示该规则作用于系统中所有网桥的所有上行或下行方向；“网桥 1—>双向”表示该规则仅作用于网桥 1 的上下行两个方向。

“内/外网地址”：定义该规则所引用的源、目的地址。提供 4 种对象形式：任意地址（等同于 any）、xxx.xxx.xxx.xxx/nn（一个网段写法为 192.168.1.0/24；一个 IP 写法为 192.168.1.100/32）、

n.n.n.n-m.m.m.m （一个连续 IP 段，写法为 172.16.1.1-172.18.1.254）、IP 群组（直接引用在“对象管理”中预先定义好的 IP 群组）。

“应用协议”：选择该规则所匹配的应用协议，可以选择一个协议组，也可以选择具体的某个协议、自定义协议、自定义协议组；带“＋”的表示协议组。自定义协议、自定义协议组需预先在对象管理配置部分定义。

“执行动作”：未创建“数据通道”时，此处将只有两个选项：允许、阻断。创建数据通道后，相

关数据通道名称将自动显示，作为动作选项引用。对应前面所选择的“数据路径”和“应用协议”选择相匹配的动作或通道即可。

数据通道可以共用，如限速“P2P 下载”和“网络电视”在两条规则里，执行动作选择同一个数据通道，则“P2P 下载”和“网络电视”共享这一数据通道。

“内网单 IP 限速”：默认数值 0，表示这条规则对内网 IP 不做单独的限速，忽略此项；如果给定内网单 IP 限速带宽数值，则表示在满足本规则动作时，同时对单个 IP 限速。上图规则 20 的整体含义为：对于内网 192.168.1.0 网段，在使用 P2P 下载类协议时，针对该网段所有 IP，下行方向的可用带宽上限为 limit-down 即 60M（本例中 limit-down 值为 60M），而具体到该网段中的每个 IP（同样是使用 P2P 下载类协议时），其个人的最大下载速度为 100kbits/s。

注：无论数据路径是选择上行方向还是下行方向，始终是先选择“内网地址”，后选择“外网地址”，如不注意，此处容易配置错误，特别是定义下行方向的规则时。

“对端发送抑制”： 根据 TCP 滑动窗口控制机制，通过调节 TCP 窗口大小，抑制对端发送速率，从而减少数据包丢弃量，达到更好的速率控制效果。由于主动抑制功能，要配合网卡的驱动定制驱动程序，才能实现这个功能，由于标准版网卡不统一，为了统一版本，不提供此功能。

“动作过后”： 该规则被匹配完后是继续还是停止。将鼠标移至行末的（帮助）查看详细说明。

多数规则选择停止匹配，当一个规则的作用域比较大，需要下一条规则继续匹配才能满足要求时，选择继续匹配。

点击提交，一条规则配置完毕，继续添加规则，重复上述过程。做完一个策略组，再创建新策略组，再逐一添加规则，形成一个新的策略组。以下是一个策略组示例：

控制策略->策略组　　系统已连续运行5天4小时10分3

选择策略组：流量控制策略组　[删除策略组]　[创建策略组>>]

序号	路径	内网地址	外网地址	协议	动作	IP限速(kb/s)	对端抑制	匹配后	添加规则>>
40	任意上行路径	myoffice	any	任意协议	允许		不抑制	停止	编辑 删除
45	任意下行路径	myoffice	any	任意协议	允许		不抑制	停止	编辑 删除
90	任意上行路径	any	any	BT扩展协议	阻断		不抑制	停止	编辑 删除
95	任意下行路径	any	any	BT扩展协议	阻断		不抑制	停止	编辑 删除
110	任意上行路径	any	any	P2P下载	limit-up		3级强度	停止	编辑 删除
130	任意上行路径	any	any	伪IE下载	limit-up		4级强度	停止	编辑 删除
210	任意下行路径	any	any	P2P下载	limit-down		不抑制	停止	编辑 删除
230	任意下行路径	any	any	伪IE下载	limit-down		不抑制	停止	编辑 删除

策略组的配置，需要做一下规划，策略组的执行，需要放在接下来的策略调度中执行，策略调度是划分时间段调用策略组，策略组的规划结合时间段，定义适当的名称标识。

3.5 策略调度

点击“添加时段”增加一个策略调度计划表，如下图：

控制策略->策略调度　　系统已连续运

缺省策略组

缺省策略组：空策略组　[修改缺省策略组]

策略调度表

编号	是否有效	日期	时刻	策略组	添加时段>>
10	有效	每周:星期一~星期日	00:00:00 ~ 23:59:59	流量控制策略組	编辑 删除

策略调度可以是按周进行，也可以按月进行，如下图：

注 1：Panabit V8.05 在策略调度中支持一个“缺省策略组”，如当前时段内没有被定义的策略调度，则系统将启用缺省策略组。用户可自行定义或修改一个策略组作为缺省策略组。缺省的策略组是：“空策略组”表示没有任何策略，系统默认是完全“允许”和放行状态。

注 2：同一个时间段，只能执行一个策略组。 策略调度中的时间设置只能是由小到大，比如 01：00—09：00，而不能是 23：00-02：00。

注 3：如需临时停止执行或启用某个策略调度，在相应策略调度行末点击“编辑”，然后在“是否有效”中选择“无效”或“有效”即可。

策略生效确认：

数据通道、策略组、策略调度三个步骤全部完成后，规则才会开始生效。确认策略生效的方法：依次点击“监控统计”—>“系统概况”—>“当前策略”，如当前策略正确显示并且相关数值有刷新，说明所建规则已生效，否则请返回“流量管理”部分重新检查并设置数据通道、策略组、策略调度三个部分。以下是策略生效的示例：

系统概况->当前策略　　系统已连续运行5天4小时16分36

Active数据通道

通道名称	通道类型	通道路径	通道带宽(kb/s)	通过流量(Bytes)	丢弃流量(Bytes)	状态
limit-up	带宽限制	任意路径	25000	84.03G	53.32G	正常
limit-down	带宽限制	任意路径	60000	201.66G	156.12G	正常

Active策略组:流量控制策略组

序号	路径	内网地址	外网地址	协议	动作	IP限速	对端抑制	匹配后	数据包
40	任意上行路径	myoffice	any	任意协议	允许		不抑制	停止	17861774
45	任意下行路径	myoffice	any	任意协议	允许		不抑制	停止	13260503
90	任意上行路径	any	any	BT扩展协议	阻断		不抑制	停止	22492052
95	任意下行路径	any	any	BT扩展协议	阻断		不抑制	停止	395201
110	任意上行路径	any	any	P2P下载	limit-up		3级强度	停止	516093069
130	任意上行路径	any	any	伪IE下载	limit-up		4级强度	停止	24466000
210	任意下行路径	any	any	P2P下载	limit-down		不抑制	停止	648816047
230	任意下行路径	any	any	伪IE下载	limit-down		不抑制	停止	39173279

4. 监控统计

监控统计，主要监视运行状态和统计数据。Panabit 流控系统可支持 4 路网桥，可针对整个系统或各个网桥进行独立的报表统计和策略管理。这部分内容，主要是查看浏览，限于篇幅，减小网站页面浏览文件大小，就不多赘述，省去截图。

4.1 分桥统计

Panabit 流控系统，策略可以对整个系统配置和分桥配置，对应的流量统计分析数据，分别有整个系统的统计数据和各桥的统计数据，选择查看。

最近 10 分钟流量分布图：最近 10 分钟内，各协议组总流量排序及百分比。
累计流量分布图：从设备上线到当前，各协议组总流量排序及百分比。
当前连接数分布图：各协议组当前 active 连接的百分比。
协议组信息：各协议组的流量参数统计数值。

最近 24 小时上行流量趋势图，图表每 5 分钟刷新一次。横坐标为最近 24 小时时间，纵坐标为速率。图底为各协议组每个 5 分钟时刻的当前速率。图表为叠加效果图，各颜色的高点减去低点即为各对应协议组的速率。

Unknown：未知协议
General： 传统协议
P2P：P2P 下载类协议
Nettv：网络电视类
Im：即时通信类
Stream：流媒体类
Voip：网络电话类
Game：网络游戏类
Stock：股票证券类
Database：数据库类
Other：其他协议类
Custom：用户自定义类

三日对比：提供最近 24 小时、前 24 小时、前 48 小时流量趋势对比。
历史图表：提供一天、一周、一月历史趋势图表。
TOP 应用：以应用协议为对象，根据具体的查询条件进行统计，查询最近 10 分钟内流量最大的 TOP 30 应用协议。

进一步了解使用 TOP 30 中各应用协议的流量报表与使用者(IP)情况，可直接点击蓝色应用协议名称，如“迅雷”。

点击“迅雷”后，首先是迅雷的“TOP 用户”统计，缺省按照累计流量列出迅雷使用者的 TOP 20 用户 IP。

进一步了解各 IP 的流量概况及连接信息，点击蓝色字体的各个 IP 即可。如查看 192.168.2.16 的 IP 档案，首先是其流量概况，然后是该 IP 详细的连接信息。

点击“趋势图表”则显示迅雷协议的最近 24 小时流量趋势报表（含 in 和 out 两个方向）以及最近 24 小时迅雷的连接趋势图。同时提供迅雷协议的“三日对比”和“历史图表”。

在线 IP 趋势：在线 IP 数的趋势图表，横坐标为时间，纵坐标为数量，图底几个数字分别为当前值（current）、平均值（average）、最大值（maximum）。

TOP IP： 以内网 IP 为统计对象，根据不同查询条件进行统计。

注 1：如需对某一段 IP 进行查询，则在“IP 范围”内分别输入起始 IP 和终止 IP 即可；如只查询一个 IP 如 192.168.1.100，则起始 IP 和终止 IP 均输入 192.168.1.100 即可。

注 2：点击各 IP，同样可对该 IP 进行档案查询，包括这个 IP 的应用概况以及连接信息。

4.2 网络接口

查询各网络接口的统计信息，网络接口仅包括数据接口。

4.3 应用协议

协议组为单位统计，对协议组所属各个应用协议进行统计排序。如选择“P2P 下载”进行查询。

说明： 对 P2P 下载类协议组进行独立统计排序，分析组内各客户端软件的应用情况。如在 P2P 下载类中，迅雷的累计流量百分比占整个 P2P 下载流量的 73%，近 10 分钟流量的比例达到 76%，说明内网用户使用的 P2P 下载工具主要集中就是迅雷，其次是 eDonkey 和 BT 等等。如需了解各应用协议的 TOP 使用者及其相关信息，点击各协议名称即可。

5. 系统维护

系统维护项，主要是系统升级，系统升级包括系统更新、特征库升级。

系统升级——是对整个引擎系统的整体升级，升级时，将有 10－15 秒的断网，请选择升级时间或下线升级。Panabit 流控引擎的系统升级包，与初始安装包，使用同一个软件安装包，在 Web 界面升级更方便。

特征库升级——特征库升级，全部是在 Web 界面升级，请经常注意检查特征库是否更新到最新，正常情况每月提供一次特征库更新，请及时到 Panabit 网站技术交流论坛特征库下载专区，查找最新特征库。特征库升级有小于 5 秒的断网时间，请选择升级时间。

系统维护，主要是主要是校对系统时间、修改口令、清除日志等，其他功能就不再赘述。请系统管理员注意上线修改口令！

附录

P2P 下载控制

Panabit 流控系统，核心是 P2P 控制的应用层流控，根据客户端软件的性质，把 P2P 应用进行了分组，如把已知的 P2P 下载客户端分为 P2P 下载类，便于策略配置时，既可以根据协议组进行带宽管理，也可以对某个协议进行带宽管理。

对 P2P 下载类进行带宽管理时，像迅雷，自身的协议或其他支持的 P2P 协议被限之后，马上就会启用，“伪 IE 下载”、“HTTP 分块传输”等，所以在配置策略时，除了对“P2P 下载”做上下行控制策略外，还需要对“伪 IE 下载”、“HTTP 分块传输”设置策略再控制，才能达到对整个 P2P 下载类的控制效果，如以下控制步骤：

第一步： 分别配置上、下行方向阻断“BT 扩展协议”，通过阻断，阻止 P2P 下载类应用主动学习探测 DHT 网络；

第二步： 分别配置上、下行方向对“P2P 下载”大类进行限速，建议下行与上行带宽比例为 5:1，根据实际情况调节；

第三步： 分别配置上、下行方向对“伪 IE 下载”、“HTTP 分块传输”限速策略；

Panabit V8.05 版本，支持自定义协议组和通道共用的配置与管理，可以把 P2P 下载类与伪 IE 下载、HTTP 分块传输自定义一个新组，这样以上第二、第三步就可以合并，使用的是自定义协议组，方便策略配置的功能；也可以把 P2P 下载和伪 IE 下载、HTTP 分块传输纳入一个共用带宽，当然一般分上下行单独配置，这是利用的带宽共用功能。

迅雷、超级旋风控制示例

1、迅雷

迅雷是支持“跨协议下载”的代表，在通讯时会使用多种协议进行数据传输：迅雷、脱兔、HTTP 分块传输、伪 IE 下载，甚至还有 FTP 和 HTTP，所以设置策略时要针对这些协议进行控制，操作步骤分两大步：

A、阻断迅雷；

B、对 HTTP 分块传输、伪 IE 下载、脱兔进行限速控制

注：以上方法对于大部分资源，已经可以达到很理想的控制效果。

下面的截图是一个示例，本例中对内网每个 IP 设定下行可用总带宽为 512kb，然后将迅雷的下载速度限制在 40kb/s ,即 5kB/s，规则生效后在"当前策略"截图如下:

当前策略组：test

通道名称	通道类型	通道方向	带宽(kbps)	状态	流量(丢弃/通过)
limit	带宽限制	下行	20	正常	73300/65425

序号	方向	源地址->目的地址	协议	动作	IP限速	匹配后	数据包
10	下行	any->any	任意协议	允许	512	继续	646
20	下行	any->any	迅雷	阻断		停止	82
30	下行	any->any	HTTP分块传输	limit		停止	73
40	下行	any->any	伪IE下载	limit		停止	40
50	下行	any->any	脱兔	阻断		停止	0

注：

1．限速迅雷相关的策略为 20、 30、 40、 50 四条。

2．10 规则动作过后 要选择 "继续匹配" ，否则下面的限速迅雷的规则一条都不会匹配，也不会生效。

3．要对迅雷做准确的限速，最好的办法是先阻断迅雷协议,然后对 HTTP 分块传输、伪 IE 下载、脱兔三种协议进行控制。本例中将迅雷和脱兔阻断，然后对 HTTP 分块传输，伪 IE 下载分别限速 20Kbits/s， 规则生效后效果非常理想。

4．如发现按以上策略设置后，迅雷的下载速度仍然很大。则需要检查并确认下载方式中是否有 FTP，如果有，将 FTP 也进行限速控制即可。

5．有时下载一个热门对象，无论怎么限速度都很快，此时一是查看该资源是否支持 HTTP 方式下载；二是在迅雷客户端查看其下载链接列表。看是否有同一网段的内网 IP，即相当于局域网内有种子，此部分流量并不经过流控设备所以不受控。

2、(腾讯)超级旋风

与迅雷相似，超级旋风也是支持跨协议下载的典型，数据传输时除少量采用自身协议外，主要采用 QQLive(QQ 直播，属于“网络电视”分类)、伪 IE 下载、HTTP 分块传输等协议，所以控制超级旋风，必须对以上几种相关协议进行策略设置。

Panabit 应用协议样本抓包方法

(2008 年 2 月)

Panabit 流控系统特征库，是保证协议识别率的关键，Panabit 研发工程师通过抓包获得协议样本，再经过特征筛选，确定具体应用的协议特征。如果使用过程中某个应用未识别，帮助抓包采集样本，Panabit 将直接分析样本，尽快提供特征库升级。采集样本参照本文档的抓包方法，取得样本后，通过邮件发送给 support@panabit.com。

一、工具软件

推荐使用：WireShark

版本号： 0.99.6

方下载地址：http://www.wireshark.org/download.html

二、抓包步骤

1、关闭所有可以访问网络的应用程序。

2、打开 WireShark，开始抓包。操作步骤为：依次点击“Capture”——“Options”——在“Interface”行选择本机访问网络所使用的网卡名称--- “Start” (窗口右下角)。

3、打开欲分析的应用软件，例如 Skype，需捕捉一个会话的完整过程，包括“登陆－选择联系人－文字聊天或通话－退出”。

4、Skype 正常应用过程中，打开 Windows 命令行程序 cmd.exe，执行 netstat －ano ，将结果拷贝到文本文件。(鼠标移入 cmd 窗口、右键“全选”、CTRL+C、创建新的 txt 文本文件、CTRL+V)

5、点击 WireShark 窗口“Capture”下的“STOP”，停止抓包。

6、点击 WireShark 窗口左上角“File”--- “Save As”保存文件。(文件后缀名为.cap，如 Skype-1.cap；并注意文件保存的位置。)

7、换另一个帐号登陆 Skype，重复以上步骤。

8、将 Skype-x.cap 各文件和步骤 4 中的文本文件同时发送邮件至：support@panabit.com

三、注意事项

1、多抓几次，要求提供不同帐号、不同访问/下载对象的完整过程包至少 3 个。

2、抓包前关闭其他可以访问网络的程序，减少无关的干扰包。

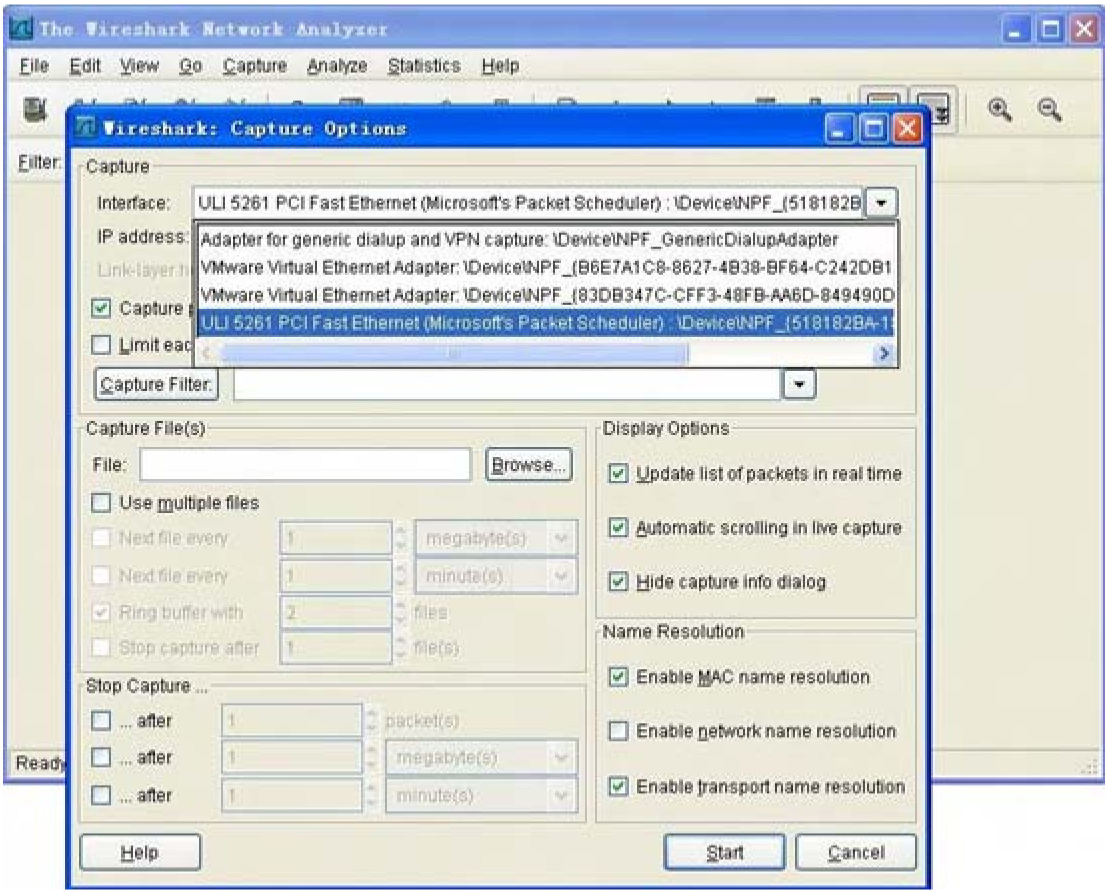
3、抓包后，为方便查看分析，请指定文件后缀名为 .cap 。

4、保证抓包的完整性，即包括登陆 —— 正常应用——退出全过程。

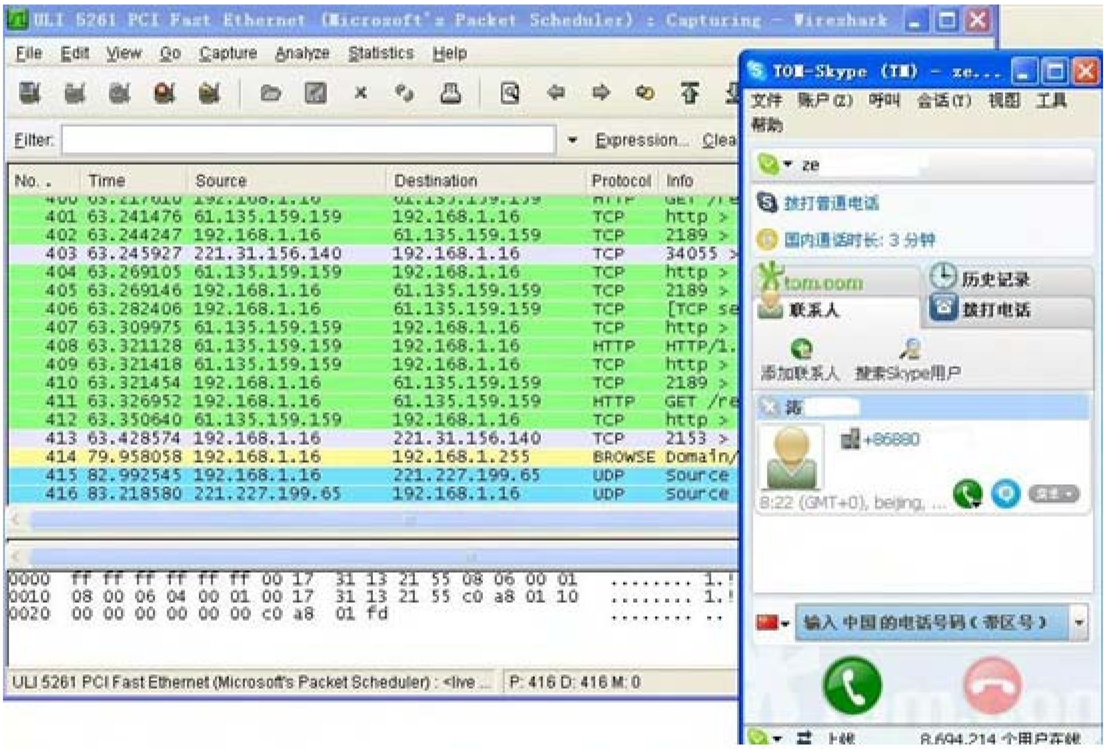
四、示例

Skype 抓包全过程：

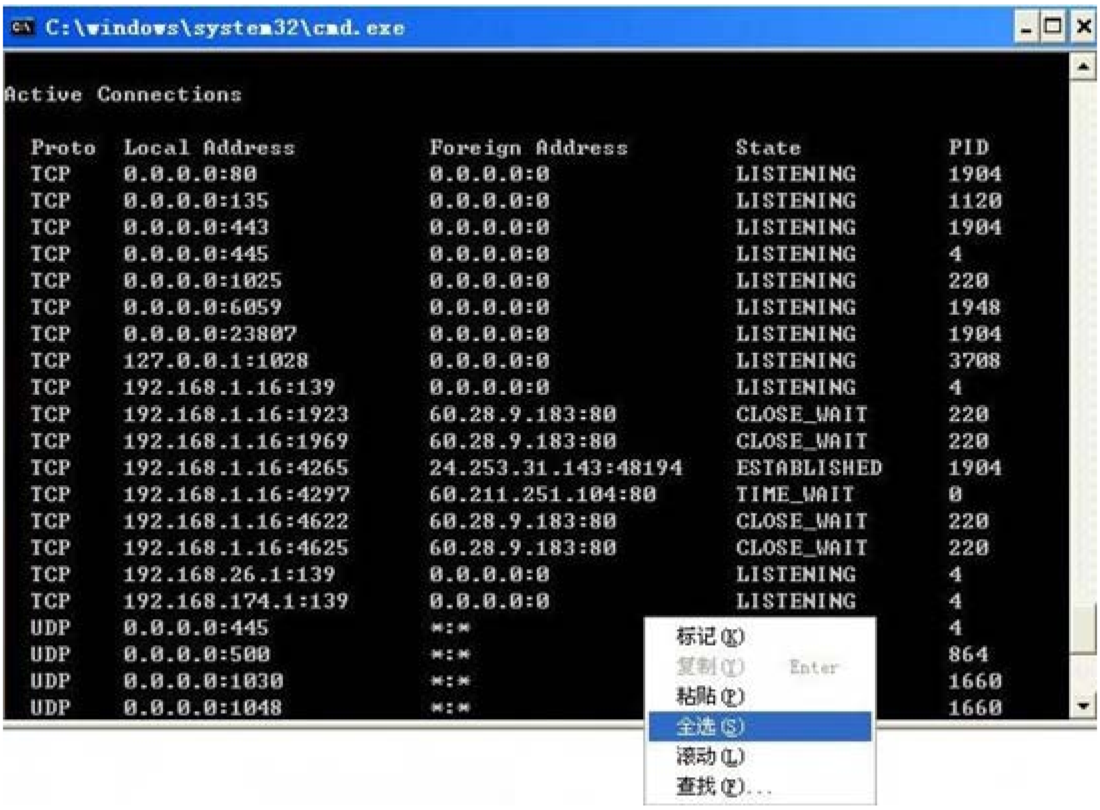
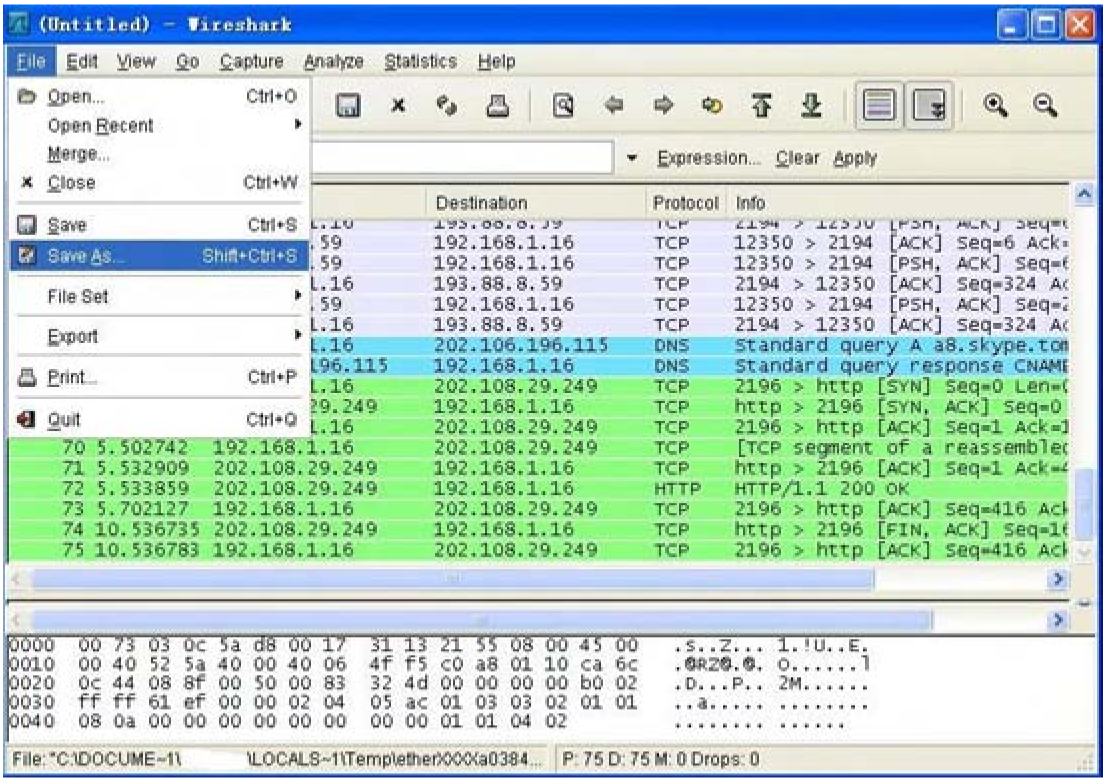
下图一、打开并执行 WireShark，依次点击“Capture”——“Options”，在最上一行“Interface”中选择本机访问网络所使用的网卡名称，点击窗口右下的“Start”。



下图二、打开 Skype，正常登陆、选中联系人、正常发送文字信息或打电话、退出。



下图三、Skype 正常登陆后的使用过程中，在 cmd 中执行 netstat －ano 并保存其信息。



下图四、将 WireShark 捕获的数据包保存为文件 Skype-1.cap。